PCT/JP99/02924
01.06.99

JP 99/02924

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

EU

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　６月　２日

出願番号
Application Number: 平成１０年特許願第１５３０６６号

出願人
Applicant (s): 日本電信電話株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

１９９９年　６月１８日

特許庁長官
Commissioner,
Patent Office 伴佐山建志

出証番号　出証特平１１－３０４３０２１

【書類名】　特許願

【整理番号】　NTTH105234

【提出日】　平成10年 6月 2日

【あて先】　特許庁長官殿

【国際特許分類】　H04K

【発明の名称】　関数のランダム性評価装置、ランダム関数生成装置、およびそのプログラム記録媒体

【請求項の数】　7

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　盛合　志帆

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　青木　和麻呂

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　神田　雅透

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　高嶋　洋一

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　太田　和夫

出証特平１１－３０４３０２１

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100066153

【弁理士】

【氏名又は名称】　草野　卓

【選任した代理人】

【識別番号】　100100642

【弁理士】

【氏名又は名称】　稲垣　稔

【手数料の表示】

【予納台帳番号】　002897

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9806848

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　関数のランダム性評価装置、ランダム関数生成装置、およびそのプログラム記録媒体

【特許請求の範囲】

【請求項１】　評価すべき関数により決まるブール関数の次数の最小値を求めて高階差分攻撃法に対する耐性を評価する高階差分攻撃耐性評価手段と、

上記評価すべき関数に対し、鍵ｋを固定してｘを入力して、素数ｐ又はｐのべき乗個の要素からなるガロア体上の多項式を用いて出力ｙ＝f_k（ｘ）を表現して、上記多項式の項数を求めて補間攻撃法に対する耐性を評価する補間攻撃耐性評価手段と、

上記評価すべき関数の入力と出力をそれぞれの部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との関係の対応関係のその平均的対応関係に対する偏よりを求めて、分割攻撃法に対する耐性を評価する分割攻撃耐性評価手段と、

評価すべき関数Ｓ（ｘ）について予め決められたΔｘに対し（Ｓ（ｘ）＋Ｓ（ｘ＋Δｘ））と出力のマスク値Γｙとの内積が１であるｘの数を２倍した値と2^n（ｎはｘのビット数）との差を求めて差分線形攻撃法に対する耐性を評価する差分線形攻撃耐性評価手段と、

の少くとも１つの評価手段を具備することを特徴とする関数のランダム性評価装置。

【請求項２】　請求項１記載の関数のランダム性評価装置において、

評価すべき関数Ｓ（ｘ）について、予め決められたΔｘ，Δｙに対しＳ（ｘ）＋Ｓ（ｘ＋Δｘ）＝Δｙを満すｘの数を求めて差分解読法に対する耐性を評価する差分解読法耐性評価手段と、

評価すべき関数についてその入力ｘとそのマスク値Γｘの内積が、関数出力値Ｓ（ｘ）とそのマスク値Γｙとの内積が等しくなるｘの数を２倍した値と、2^nとの差を求めて、線形解読法に対する耐性と評価する線形解読法耐性評価手段との少くとも１つを備えることを特徴とする関数のランダム性評価装置。

【請求項３】　代数構造の異なる複数の関数を組合わせた複数のパラメータ

を有する候補関数群を生成する候補関数生成手段と、

上記各候補関数群のそれぞれについて、解読攻撃に対する耐性を評価する耐性評価手段と、

上記耐性評価された候補関数群の耐性の強いものを選出する選択手段と、

を具備するランダム関数生成装置。

【請求項４】　請求項３記載のランダム関数生成装置において、

上記代数構造の異なる関数の１つは差分解読法及び線形解読法に対する各耐性が強いものであることを特徴とするランダム関数生成装置。

【請求項５】　請求項３又は４記載のランダム関数生成装置において、

上記耐性評価手段は、上記候補関数により決まるブール関数の次数の最小値を求めて高階差分攻撃法に対する耐性を評価する高階差分攻撃耐性評価手段と、

上記候補関数に対し、鍵ｋを固定してｘを入力して、素数ｐ又はｐのべき乗個の要素からなるガロア体上の多項式を用いて出力$y = f_k(x)$を表現して、上記多項式の項数を求めて、補間攻撃法に対する耐性を評価する補間攻撃耐性評価手段と、

上記候補関数の入力と出力をそれぞれの部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との関係の対応関係のその平均的対応関係に対する偏よりを求めて、分割攻撃法に対する耐性を評価する分割攻撃耐性評価手段と、

上記候補関数Ｓ（ｘ）について予め決められたΔｘに対し（Ｓ（ｘ）＋Ｓ（ｘ＋Δｘ））と出力のマスク値Γｙとの内積が１であるｘの数を２倍した値と2^n（ｎはｘのビット数）との差を求めて差分線形攻撃法に対する耐性を評価する差分線形攻撃耐性評価手段と、

の少くとも１つよりなることを特徴とするランダム関数生成装置。

【請求項６】　代数構造の異なる複数の関数を組合わせた複数のパラメータを有する候補関数群を生成する候補関数生成処理と、

上記各候補関数について、各パラメータに各種値を設定し、各種入力値に対する出力値をそれぞれ演算する演算処理と、

上記演算処理の結果を記憶手段に記憶する処理と、

上記記憶手段に記憶された値を用いて上記各候補関数のそれぞれについて、解読攻撃に対する耐性を評価する耐性評価処理と、

その耐性評価処理結果にもとづき、耐性の強い候補関数を選択出力する選択処理と、

をコンピュータにより実行させるプログラムを記録した記録媒体。

【請求項７】　請求項６記載の記録媒体において、

上記耐性評価処理は、

上記候補関数により決まるブール関数の次数の最小値を求めて高階差分攻撃法に対する耐性を評価する高階差分攻撃耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残し他を除去する処理と、

その残された候補関数Ｓ（ｘ）について、予め決められたΔｘ，Δｙに対しＳ（ｘ）＋Ｓ（ｘ＋Δｘ）＝Δｙを満すｘの数を求めて差分解読法に対する耐性を評価する差分解読法耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残し、他を除去する処理と、

その残された候補関数についてその入力ｘとそのマスク値Γｘの内積が、関数出力値Ｓ（ｘ）とそのマスク値Γｙとの内積が等しくなるｘの数を２倍した値と2^nとの差を求めて、線形解読法に対する耐性を評価する線形解読法耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残し、他を除去する処理と、

その残りの候補関数Ｓ（ｘ）について予め決められたΔｘに対し（Ｓ（ｘ）＋Ｓ（ｘ＋Δｘ））と出力のマスク値Γｙとの内積が１であるｘの数を２倍した値と2^n（ｎはｘのビット数）との差を求めて差分線形攻撃法に対する耐性を評価する差分線形攻撃耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残し、他を除去する処理と、

その残された候補関数の入力と出力をそれぞれの部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との関係の対応関数のその平均的対応関係に対する偏よりを求めて、分割攻撃法に対する耐性を評価する分割攻撃耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残し、他を除去する処理と、

その残された候補関数に対し、鍵ｋを固定してｘを入力して、素数ｐ又はｐのべき乗個の要素からなるガロア体上の多項式を用いて出力ｙ＝f_k（ｘ）を表現して、上記多項式の項数を補間攻撃法に対する耐性を評価する補間攻撃耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残して他を除去する処理とからなることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、例えば暗号装置等へ適用され、入力に対する出力が不規則に生成され、その動作を解析することが困難であるような関数を得るために、いくつかのランダム性指標を満たすかどうかを評価する装置、ランダム性指標を満たすと評価されたランダム関数を生成する装置およびそのプログラム記録媒体に関する。

【０００２】

【従来の技術】

データを秘匿するためには暗号化技術が有効である。暗号化の方法は秘密鍵暗号方式と公開鍵暗号方式がある。一般に公開鍵暗号技術の方が安全性の証明技術の研究が進んでいるので、安全性の限界を知りつつ利用することができる。しかし、秘密鍵暗号については安全性の証明技術は確立されておらず、暗号攻撃が発見されると、その都度、個別に対処する必要が生じる。

【０００３】

高速かつ安全な秘密鍵暗号を構成するために、暗号化対象のデータを適当な長さのブロックに分割し、そのブロック毎に暗号化する方法をブロック暗号と呼ぶ。通常ブロック暗号は暗号学的にあまり強くない関数を、平文に対し複数回繰り返し適用することにより安全性を高めている。この、あまり強くない関数をＦ関数と呼ぶ。

【０００４】

Ｆ関数の構成要素として、Ｓ－ｂｏｘと呼ばれる、入力に対する出力が不規則

に生成され、その動作を解析することが困難であるような関数を用いることが一般的となっている。従来は、Ｓ－ｂｏｘを構成する際に、安全性の根拠として、例えば、暗号化したデータの各ビットの０，１の出現確率が統計的に１／２となる程度のことしか考えられておらず、ブロック暗号の理論的な安全性の根拠として不十分であった。

【０００５】

実際、上記の基準を満たすブロック暗号に対する攻撃法として、差分解読法が文献「E.Biham , A.Shamir : “Differential Cryptanalysis of DES-like Cryptosystems, ” Journal of Cryptology , Vol.４, No. １, pp. 3-72」で、線形解読法が文献「M.Matsui : “Linear Cryptanalysis Method for DES Cipher, ” Advances in Cryptology－EUROCRYPT'93 (Lecture Notes in Computer Science 765), pp.386-397, Springer-Verlag , 1994」で提案され、多くのブロック暗号がこれらの解読法により解読できることがわかり、安全性の基準の見直しが必要となった。

【０００６】

差分解読法や線形解読法が提案されてからブロック暗号にはこれらの解読法に対して強いことが要求されるようになった。そこで、これらの解読法に対して耐性があることを示す指標として、それぞれ最大平均差分確率や最大平均線形確率が文献「松井　充：『ブロック暗号の差分解読法と線形解読法に対する証明可能安全性について』第１８回情報理論とその応用シンポジウム予稿集（Ｃ－２－５），pp. 175-178 」（以下「SITA 95-C-2-5 」と略す）で提案された。これらの指標は小さいほどそれぞれの解読法に対する耐性があることが示されている。

【０００７】

さらに近年、差分解読法や線形解読法に対する耐性のある暗号でも、これ以外の解読法によって解読されることが指摘され、さらに安全性の基準の見直しが必要となった。具体的には、文献「T.Jakobsen, L.R.Knudsen : “The Interpolation Attack on Block Cipher, ” Fast Software Encryption Workshop(FSE4) (Lecture Notes in Computer Science 1267) , pp.28-40, Springer Verlag,1997」（以下文献Ａと記す）において、差分解読法や線形解読法に対する耐性のある

暗号でも、高階差分攻撃や補間攻撃によって解読される暗号があることが示された。

【０００８】

さらに高階差分攻撃や補間攻撃以外にも文献「C.Harpes, J.L.Massey：“Partitioning Cryptanalysis,” Fast Software Encryption Workshop(FSE4) (Lecture Notes in Computer Scinece 1267), pp.13-27, Springer Verlag, 1997」において線形解読法を一般化した分割攻撃が提案され、この攻撃に対しても十分な耐性があることを保証することが必要となっている。

【０００９】

【発明が解決しようとする課題】

差分解読法、線形解読法に対する安全性を保証する技術が、一部のブロック暗号の構成法に対して確立しているのに対して、高階差分攻撃、補間攻撃、分割攻撃に対して完全に耐性があることを保証する技術は現時点では確立していない。すなわち、暗号がこれらの攻撃に対して安全であるためにランダム関数、いわゆるＳ－ｂｏｘが満たすべき必要十分条件は明らかになっていない。

【００１０】

しかし、Ｓ－ｂｏｘを設計する上で、これらの攻撃法に対しても十分な強度をもつようにすることは重要な課題である。

そこで、この発明の一目的は、上記の各攻撃法に対し、その攻撃法に対する強度と深く関わる指標を見い出し、その指標が（各攻撃に対して強いことを保証する必要十分条件を満たさないまでも、）各攻撃に対して耐性をもつための必要条件を示し、それらの一部または全ての条件を満たすようなＳ－ｂｏｘ評価装置を提供することにある。

【００１１】

さらに、この発明の他の目的はこれらの強度指標を満たすＳ－ｂｏｘの構成装置とそのプログラム記録媒体を提供することにある。

【００１２】

【課題を解決するための手段】

第１発明によれば、高階差分攻撃法、補間攻撃法、分割攻撃法、に対する強度

指標とそれらの強度指標が各解読法に対する耐性をもつための必要条件を設定し、候補となる関数群について上記の一部または全ての条件が満たされるかどうかを評価し、必要に応じて上記の一部または全ての条件が満たされるものを選ぶ。更に、この選ばれたものは差分解読法、線形解読法の少くとも一方に対して耐性が強いことが評価される。

【００１３】

以下に差分解読法、線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法に対する強度指標とそれらの強度指標が各解読法に対する耐性をもつための必要条件を述べる。以下ではｎ，ｍを任意の自然数とし、Ｓ－ｂｏｘ（ランダム関数）としてｎビット入力、ｍビット出力の関数Ｓ：ＧＦ(2)^{n}→ＧＦ(2)^{m}を考える。ＧＦ(2)^{n}は全てのｎビットデータの集合を示す。

【００１４】

差分解読法に対する耐性をもつための必要条件

Ｓ－ｂｏｘの差分解読法に対する耐性を示す指標として差分攻撃指標を定義し、その測定方法を述べ、差分解読法に対する耐性をもつための必要条件を示す。

差分解読法では、Ｓ－ｂｏｘの２つの入力の差分（入力差分値）に対する出力の差分（出力差分値）を観測し、大きな偏りがある場合に、これを利用して暗号全体の解読につなげることができる。

【００１５】

Ｓ－ｂｏｘの入力をｘ、入力差分値をΔｘ、出力差分値をΔｙとすると、ある入力差分値Δｘと、出力差分値Δｙに対して、全てのｎビット入力ｘのうち、式（１）を満たすｘの個数をδ_{s}（Δｘ，Δｙ）とする。但し、通常、“＋”はビット毎の排他的論理和（ＸＯＲ）で定義される。文献「X.Lai, J.L.Massey, and S.Murphy."Markov Ciphers and Differential Cryptanalysis." In D.W.Davies, editor, Advances in Cryptology-EUROCRYPT '91, Volume 547 of Lecture Notes in Computer Science,pp. 17-38. Springer-Verlag, Berlin, Heidelberg, New York, 1991」で述べられているように、一般的な逆元がある二項演算を用いて定義できる。

【００１６】

$$S(x)+S(x+\Delta x)=\Delta y \qquad (1)$$

これを書き換えると、$\delta_s(\Delta x, \Delta y)$は式（２）のように書ける。但し、#｛ｘ｜条件式｝は条件式を満たすｘの個数とする。

$$\delta_s(\Delta x, \Delta y)=\#\{x\in GF(2)^n \mid (S(x)+S(x+\Delta x))=\Delta y \qquad (2)$$

入力差分値として０を除く全てのｎビットデータΔｘと出力差分値として全てのｍビットデータΔｙに対して、式（２）より$\delta_s(\Delta x, \Delta y)$を計算することができる。このうち最も大きい値をとるΔｘとΔｙの組合せが差分解読法における脆弱点となるため、$\delta_s(\Delta x, \Delta y)$の最大値が小さいほど差分解読法に対する耐性が大きいということになる。よって式（３）で示される差分解読指標Δ_sが小さいことが差分解読法に対して耐性をもつための必要条件となる。

【００１７】

$$\Delta_s=\max \delta_s(\Delta x, \Delta y) \qquad (3)$$

ｍａｘはΔｘ≠０、Δｙの全組合せの中から最大値を選ぶという条件とする

線形解読法に対する耐性をもつための必要条件

Ｓ－ｂｏｘの線形解読法に対する耐性を示す指標として線形攻撃指標を定義し、その測定方法を述べ、線形解読法に対する耐性をもつための必要条件を示す。

【００１８】

線形解読法では、Ｓ－ｂｏｘの入力値と出力値のビット単位での任意の線形和（排他的論理和）を観測し、大きな偏りがある場合に、これを利用して暗号全体の解読につなげることができる。

Ｓ－ｂｏｘの入力をｘ、入力マスク値をΓｘ、出力マスク値をΓｙとすると、ある入力マスク値Γｘと出力マスク値Γｙに対して、式（４）で定義されるλ_s（Γｘ，Γｙ）が計算できる。但し、通常、“・”は内積で定義される。ｘ・Γｘの意味は、マスク値Γｘ中の“０”に対応するｘ中のビット値は無視し、“１”に対応するｘ中のビット値のみを有効として、それらの和をとることを表わす。すなわち、$x\cdot\Gamma x=\Sigma x_i$（ΣはΓｘ中の第ｉビットが“１”の総和）但し$x=(x_{n-1},\cdots x_0)$とする。

【００１９】

λ_s（Γｘ，Γｙ）

$$= | 2 \times \#\{x \in GF(2)^n \mid x \cdot \Gamma x = S(x) \cdot \Gamma y\} - 2^n | \quad (4)$$

入力マスク値として全てのｎビットデータΓｘと、出力マスク値として０を除く全てのｍビットデータΓｙに対して、式（４）よりλ_s（Γｘ，Γｙ）を計算することができる。このうち最も大きい値をとるΓｘとΓｙの組合せが線形解読法における脆弱点となるため、λ_s（Γｘ，Γｙ）の最大値が小さいほど線形解読法に対する耐性が大きいということになる。よって式（５）で示される線形解読指標Λ_sが小さいことが線形解読法に対して耐性をもつための必要条件となる。

【００２０】

$$\Lambda_s = \max \lambda_s (\Gamma x, \Gamma y) \quad (5)$$

ｍａｘはΓｘ，Γｙ≠０の全ての組合わせの中から最大値を選ぶという条件とする

高階差分攻撃法に対する耐性をもつための必要条件

Ｓ－ｂｏｘの高階差分攻撃法に対する耐性を示す指標として高階差分攻撃指標を定義し、その測定方法を述べ、高階差分攻撃法に対する耐性をもつための必要条件を示す。

【００２１】

高階差分攻撃法とは、暗号化途中の中間出力を入力に関して高階差分をとると、鍵によらない定数になることを利用した攻撃法である。暗号化途中の任意の中間データの任意のビットは、入力に関するブール多項式で表現できる。そのブール多項式の次数がｄであった時、ｄ＋１階差分をとると、その結果は鍵によらない定数になることから、これまでに、ブール多項式の次数が低い暗号に対する攻撃が前記文献Ａで報告されている。

【００２２】

Ｆ関数のブール多項式表現の次数が低ければ、Ｆ関数の繰り返し回数が十分多くないと暗号全体のブール多項式表現の次数も高くならず、解読される危険性が高い。よって、Ｆ関数の構成要素であるＳ－ｂｏｘのブール多項式表現の次数も高いことが、Ｆ関数の繰り返し回数を増やすことなくその暗号が高階差分攻撃に対して安全にするための必要条件といえる。

【００２３】

Ｓ－ｂｏｘＳ：ＧＦ（２）^{n}→ＧＦ（２）^{m}；ｘ→Ｓ（ｘ）に対し、

ｙ＝Ｓ（ｘ），

ｘ＝（x_{n-1}，x_{n-2}，…，x_{0}）∈ＧＦ（２）^{n}，

ｙ＝（y_{m-1}，y_{m-2}，…，y_{0}）∈ＧＦ（２）^{m}

とする。また、変数集合Ｘ＝｛x_{n-1}，x_{n-2}，…，x_{0}｝を定義する。この時、y_i＝S_i（ｘ）なるブール関数S_i：ＧＦ（２）^{n}→ＧＦ（２）；ｘ→S_i（ｘ）を定義し、変数集合Ｘに関するブール関数S_i（０≦ｉ≦ｍ－１）の次数を deg_X S_i とする。以下のように deg_X S_i （０≦ｉ≦ｍ－１）の最小値をdeg_X Ｓとし、これが高階差分攻撃指標となる。

【００２４】

$$deg_X\ S = min\ (deg_X\ S_i) \qquad (6)$$

ｍｉｎは０≦ｉ≦ｍ－１を条件とする

高階差分攻撃に対して安全であるためにＳ－ｂｏｘが満たすべき必要条件は、deg_X Ｓが大きい値をもつことである。Ｓが全単射であれば、deg_X Ｓの最大値はｎ－１であることが知られている。

補間攻撃法に対する耐性をもつための必要条件

Ｓ－ｂｏｘの補間攻撃法に対する耐性を示す指標として補間攻撃指標を定義し、その測定方法を述べ、補間攻撃法に対する耐性をもつための必要条件を示す。

【００２５】

補間攻撃の原理は次の通りである。鍵ｋを固定した時、暗号文ｙは、平文ｘについてのＧＦ（ｑ）上多項式f_k（ｘ）を用いてｙ＝f_k（ｘ）と表すことができる。但し、ｑは素数または素数のべき乗である。f_k（ｘ）に含まれるｘについての項数がｃである時、異なるｃ組の平文とそれに対する暗号文の組（x_i，y_i）（１≦ｉ≦ｃ）が与えられれば、ラグランジェ補間公式などにより、f_k（ｘ）を構成することができる。これにより、任意の平文ｘに対する暗号文を得ることができる。

【００２６】

f_k（ｘ）に含まれる項数が多いほど、ＧＦ（ｑ）上多項式表現f_k（ｘ）を用いた補間攻撃に必要な平文と暗号文の組は多くなり、攻撃は困難または不可能

となる。

Ｓ－ｂｏｘのＧＦ（ｑ）上多項式表現に含まれる項数が少ないと、暗号全体のＧＦ（ｑ）上多項式表現に含まれる項数が少なくなる可能性がある。もちろん、Ｓ－ｂｏｘのＧＦ（ｑ）上多項式表現に含まれる項数が多くても、暗号全体を構成する上で項が打ち消し合い、暗号全体のＧＦ（ｑ）上多項式表現に含まれる項数が少なくならないよう注意する必要はあるが、これは暗号構成法に関することであり、Ｓ－ｂｏｘの補間攻撃指標としてはＧＦ（ｑ）上多項式表現に含まれる項数が多いことが補間攻撃法に対する耐性をもつための必要条件となる。Ｓ－ｂｏｘの関数ＳのＧＦ（ｑ）上多項式表現に含まれる項数を coeff_q Ｓとし、これをＧＦ（ｑ）上多項式表現を利用する補間攻撃の攻撃指標とする。

【００２７】

補間攻撃は想定されるｑとして取りうる場合の数だけ攻撃が存在するので、なるべく多くのＧＦ（ｑ）上多項式表現に対してその項数 coeff_q Ｓを計算し、それらが小さい値をとらないことを確認する必要がある。

分割攻撃法に対する耐性をもつための必要条件

Ｓ－ｂｏｘの分割攻撃法に対する耐性を示す指標として分割攻撃指標を定義し、その測定方法を述べ、分割攻撃法に対する耐性をもつための必要条件を示す。

【００２８】

分割攻撃法では、平文集合全体のある部分集合と暗号文集合全体のある部分集合に成り立つ何らかの指標を観測し、大きな偏りが見い出される場合に、これを利用して暗号全体の解読につなげることができる。この「何らかの指標Ｉ」としては、文献「C.Harpes, J.L.Massey：“Partitioning Cryptanalysis,”Fast Software Encryption Workshop(FSE4) (Lecture Notes in Computer Science 1267)，pp.13-27, Springer Verlag,1997」ではpeak imbalanceとsquared Euclidean imbalanceが例として挙げられている。

【００２９】

文献「浜出　猛，横山尚史，島田　徹，金子敏信：『ＤＥＳ暗号に対するpartitioning cryptanalysis of DES』，１９９８年暗号と情報セキュリティシンポジウム予稿集（SCIS'98-2.2.A)」において、Ｓ－ｂｏｘの入出力集合に対して観

測される偏りを利用して、暗号全体の攻撃に成功していることから、Ｓ－ｂｏｘの入出力集合に対して同様に定義された分割攻撃指標が暗号全体が分割攻撃法に対する耐性をもつための必要条件であることが分かる。

【００３０】

Ｓ－ｂｏｘの全入力集合をｑ分割し、各部分集合をF_0，F_1，F_{q-1}、全出力集合をｍ分割し、各部分集合をG_0，G_1，G_{m-1}とする。各部分集合に含まれる要素数は全て等しいとする。入力ｘを各部分集合の添字｛０，１，…，ｑ－１｝に写像する関数ｆを入力の分割関数、出力ｙを｛０，１，…，ｍ－１｝に写像する関数ｇを出力の分割関数と呼ぶ、つまりｘがどの部分集合に属するかを示す関数がｆであり、ｙがどの部分集合に属するかを決める関数がｇである。分割Ｆ，Ｇをそれぞれ

$$F=\{F_0, F_1, \cdots, F_{q-1}\},$$

$$G=\{G_0, G_1, \cdots, G_{m-1}\}$$

とすると、Ｓ－ｂｏｘの分割対（Ｆ，Ｇ）の偏りI_s（（Ｆ，Ｇ））は式（７）で与えられる。

【００３１】

$$I_s((F, G))=(1/q)\ \Sigma_{i=0}^{q-1}\ I(g(S(x))\mid f(x)=i) \quad (7)$$

これがＳ－ｂｏｘの分割攻撃指標であり、０～１の何れかの値をとり、その値と１／２との差が小さいことが分割攻撃法に対する耐性をもつための必要条件となる。

次に、第２発明について述べる。文献「T.Jakobsen, L.R.Knudsen: “The Interpolation Attack on Block Cipher, ” Fast Software Encryption Workshop(FSE4) (Lecture Notes in Computer Science 1267) , pp.28-40, Springer Verlag , 1997」で挙げられている例により、差分解読法や線形解読法に対する耐性をもつ関数として、ある代数構造をもつ関数を選んでＳ－ｂｏｘとして採用し、その代数構造を壊さない演算のみと組み合わせて暗号全体を構成すると、高階差分攻撃法や補間攻撃法などの代数攻撃法により容易に解読されることが分かっている。よって、第２発明の実施例は差分解読法や線形解読法に対する耐性をもつ関数と、その関数の代数構造と異なる代数構造をもつ関数を組み合わせた（例えば

、関数の合成など）関数を候補の関数群として選び、その関数群のそれぞれについてその解読に対する耐性を評価し、耐性の強いものを選択する。

【００３２】

なお、この発明における候補関数群の選び方は必ずしも以上の手段に限定される必要はない。

作用

従来は、Ｓ－ｂｏｘ設計（ランダム性評価）の指針として、例えば、暗号化したデータの各ビットの０，１の出現確率が統計的に１／２となる程度のことしか考えられておらず、暗号全体の攻撃に直結する評価指標が用いられることは少なかったが第１発明によれば、差分解読法、線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法、その他想定される攻撃法に対する耐性をもつかどうか評価する装置を加えることで、上記の暗号攻撃に対する高い安全性をもつ暗号を設計できることが期待される。

【００３３】

このようにして攻撃に対する耐性が評価されたが、耐性の強いランダム関数を生成するには、候補となる関数群をどのように選ぶかという問題点が生じる。膨大な関数の中から上記の条件を満たす関数を選ぶのには多くの計算量を必要とするためである。

これを、第２発明の実施例によれば差分解読法や線形解読法に対する耐性をもつ関数と、その関数の代数構造と異なる代数構造をもつ関数を組み合わせた（例えば、関数の合成など）関数を候補の関数群として選ぶことで、少ない候補の中から、差分解読法や線形解読法だけでなく、高階差分攻撃法、補間攻撃法などの代数的構造を利用した攻撃法に対する耐性をもつ関数を効率的に絞り込むことができる。

【００３４】

【発明の実施の形態】

図１にこの発明によるランダム関数生成装置、関数のランダム性評価装置の実施例の機能構成を示す。入力手段１により生成しようとする関数のもととなるもの、そのパラメータなどが入力され、候補関数生成手段２において、入力手段１

の入力に応じた候補関数が生成され、そのパラメータ値と入力値とこれらにもとづく演算結果（出力値）とが記憶部３に記憶される。記憶部３に記憶された各種データが読出され、差分解読法耐性評価手段４、線形解読法耐性評価手段５、高階差分攻撃法耐性評価手段６、補間攻撃法耐性評価手段７、分割攻撃法耐性評価手段８、その他の指標評価手段９でそれぞれ耐性評価、指標評価などがなされる。その各結果にもとづき、耐性の強い候補関数が関数選択手段１０で選択され、記憶部１１に記憶され、所要のものが出力手段１２から出力される。

【００３５】

この発明による関数がランダム性評価装置においては、入力手段１から評価されるべき関数が、各手段４～９に入力されて、ランダム性評価が行われる。

この実施例では、特願平１０－０１３５７２データ変換装置中のＳ－ｂｏｘとして用いる８ビット入出力のＳ－ｂｏｘの設計法について述べる。

まず、Ｓ－ｂｏｘの候補関数として、例えば図２に示すように関数Ｐ（ｘ，ｅ）を生成する手段２１と、Ｐ（ｘ，ｃ）と代数構造を異にする関数Ａ（ｙ，ａ，ｂ）を生成する手段２２とが合成されたものとする。

【００３６】

$S:GF(2)^8 \rightarrow GF(2)^8 ; x \rightarrow A((P(x, e)), a, b)$，

但し

$$P(x, e) = x^e \text{ in } GF(2^8) \quad (8)$$

$$A(y, a, b) = ay + b \pmod{2^8} \quad (9)$$

である。Ｐ（ｘ，ｅ）はガロア体ＧＦ（2^8）上で定義されるべき乗関数である。この時、パラメータａ，ｂ，ｅは０以上２５５以下の任意の自然数という自由度がある。このうち、パラメータａ，ｂのハミング重みを３以上５以下に限定し、つまりａ，ｂは各８ビットであるがそのうち“１”（又は“０”）が３ビット以上５ビット以下であり、さらにＳ－ｂｏｘが全単射であること、差分解読法、線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法に対する耐性があるための必要条件を満たすかどうかを評価し、パラメータａ，ｂ，ｅを絞り込んでいく。

【００３７】

その例、つまりこの発明の装置の一実施例の処理手順を図３に示す。なお、実施例はこの例に限られない。Ｓ－ｂｏｘの候補とする関数の選び方には自由度がある。またＳ－ｂｏｘの設計指標も数多くあり、その優先順位や候補関数の絞り込みの順序など、多くの自由度がある。

図３において、ステップＳ１で候補関数Ｓが全単射であるかを評価する。パラメータａが奇数、ｅが$2^8-1=255$と互いに素である時、関数Ｓは全単射になるので、これらを満たすパラメータを選択し、満たさないものは候補から除く。この処理は図１中の手段９により行う。あるいはパラメータａは入力手段１で奇数のみを入力することで得る。

【００３８】

ｅのハミング重みと式（６）で表わせる高階差分攻撃指標 deg_x Ｓとが等しいことが知られている。そこでステップＳ２で、残りの候補関数Ｓの高階差分攻撃指標 deg_x Ｓの条件を満たすため、ここでは deg_x Ｓの最大値、つまりｅのハミング重みが７になるものを選択する。これを満たさないものは候補から除く。

ステップＳ３で残りの関数Ｓの差分攻撃指標Δ_Sの条件を満たすため、関数Ｓの差分攻撃指標Δ_Sが最小となるものを選択する。これを満たさないものは候補から除く。

【００３９】

ステップＳ４で残りの候補関数Ｓの線形攻撃指標Λ_Sの条件を満たすため、関数Ｓの線形攻撃指標Λ_Sが最小となるものを選択する。これを満たさないものは候補から除く。

ステップＳ５では以下の式で定義される関数Ｓの差分線形攻撃指標Ξ_Sが最小となるものを選択する。これを満たさないものは候補から除く。

【００４０】

$$\xi_S(\Delta x, \Gamma y)$$

$$=\left|\,2\times\#\left\{x\in GF(2)^8 \mid (S(x)+S(x+\Delta x))\cdot \Gamma y=1\right\}-2^8\,\right|$$

$$\Xi_S=\max \xi_S(\Delta x, \Gamma y)$$

ｍａｘは$\Delta x\neq 0$，$\Gamma y\neq 0$の全組合わせの中から最大値を選ぶという条件とする

ｋをｎ以下の自然数とした時、

【００４１】

【数１】

$$S:GF(2)^n \rightarrow GF(2)^n : x \rightarrow x^{2^k} \text{ in } GF(2^n)$$、

または$$S:GF(2)^n \rightarrow GF(2)^n : x \rightarrow x^{2^k+1} \text{ in } GF(2^n)$$の時、

この指標が最大値2^nをとることが示される。これが直接何らかの攻撃に結び付く例はまだ報告されていないが、この指標についてもなるべく小さい値をとる（顕著な偏りがない）ことが望ましいため、パラメータの選択基準に加えた。

この結果、以下のパラメータまで絞り込める。

【００４２】

（ａ，ｂ）＝（97,97），(97,225),(225,97)，(225,225)

ｅ＝ 127,191,223,239,247,251,253,254

次に、ステップＳ６で残りの候補、関数Ｓの分割攻撃指標I_s（（Ｆ，Ｇ））の条件を満たすため、上記のパラメータの全ての組み合わせのうち、関数Ｓの分割攻撃指標I_s（（Ｆ，Ｇ））が１／２に近いかどうかを確認する。１／２との差が大きいものがあれば候補から除く。

【００４３】

ステップＳ７で更に残りの候補関数ＳのＧＦ（2^8）上の多項式を利用する補間攻撃指標 $coeff_q$ Ｓ（ただしｑ＝2^8）の条件を満たすため、上記パラメータの全ての組み合わせのうち、関数ＳのＧＦ（2^8）上の多項式を利用する補間攻撃指標 $coeff_q$ Ｓが大きいかどうかを確認する。小さいものがあれば候補から除く。

【００４４】

ステップＳ８では、2^8+1以上2^9以下の全ての素数ｐについて、関数ＳのＧＦ（ｐ）上の多項式を利用する補間攻撃指標 $coeff_p$ Ｓの条件を満たすため、関数ＳのＧＦ（ｐ）上の多項式を利用する補間攻撃指標 $coeff_p$ Ｓが大きいかどうか、この例では最大値をとるかを確認する。小さいものがあれば候補から除く。

【００４５】

以上の評価の結果、以下のパラメータの組み合わせ（全３２種類）が残る。

（ａ，ｂ）＝ (97,97),(97,225),(225,97),(225,225)

ｅ＝ 127,191,223,239,247,251,253,254

この結果はステップＳ５での結果と同一である。つまりこの例ではステップＳ５で既に本実施例で考慮するあらゆる攻撃法に対しても強い関数が得られたことになる。

【００４６】

このようにして選択された３２個の関数は上記の評価基準における強度は等しいので、Ｓ－ｂｏｘとしてどの関数を選んでもよい。

Ｓ－ｂｏｘの評価として、又は関数生成において、解読計算量が現実的に計算可能な値から各種の攻撃に対する各評価指標の基準が決定され、これらの基準を全て越えれば、そのランダム性は合格、あるいはその関数は使用してもよいと、その要求されるランダム性の程度、つまり各種の攻撃に対する強さに応じて各指標に対するしきい値（基準値）が決定される。

【００４７】

【発明の効果】

以上述べたように、この発明によれば、暗号装置等の構成要素となるＳ－ｂｏｘ関数のランダム性評価方法およびその装置において、従来の評価方法に加えて、差分解読法、線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法、その他想定される攻撃法に対する耐性をもつかどうか評価する手段を加えることで、ランダム性の評価を正しく行え、かつ上記の暗号攻撃に対する高い安全性をもつ暗号が設計できる。

【００４８】

さらに、候補となる関数群を差分解読法や線形解読法に対する耐性をもつ関数と、その関数の代数構造と異なる代数構造をもつ関数を組み合わせた関数を候補の関数群として選ぶことで、少ない候補の中から、差分解読法や線形解読法だけでなく、高階差分攻撃法、補間攻撃法などの代数的構造を利用した攻撃法に対する耐性をもつ関数を効率的に絞り込むことができる。

【００４９】

また図３に示したような手順で絞り込みを行うと、少ない演算量で効率的に絞り込みを行うことができる。

また、候補となる関数群をランダムに選ぶのではなく、よく知られた異なる代数構造をもつ関数の組み合わせから選ぶことで、Ｓ－ｂｏｘにトラップドア（設計者だけがその暗号を解読できるような秘密のしかけ）がないことも示しやすい。

【図面の簡単な説明】

【図１】

この発明によるランダム関数生成装置、関数のランダム性評価装置の機能的構成例を示すブロック図。

【図２】

この発明によるランダム関数生成装置の基本構成の例を示すブロック図。

【図３】

この発明によるランダム関数生成装置の実施例の処理手順の例を示す流れ図。

【書類名】　図面

【図１】

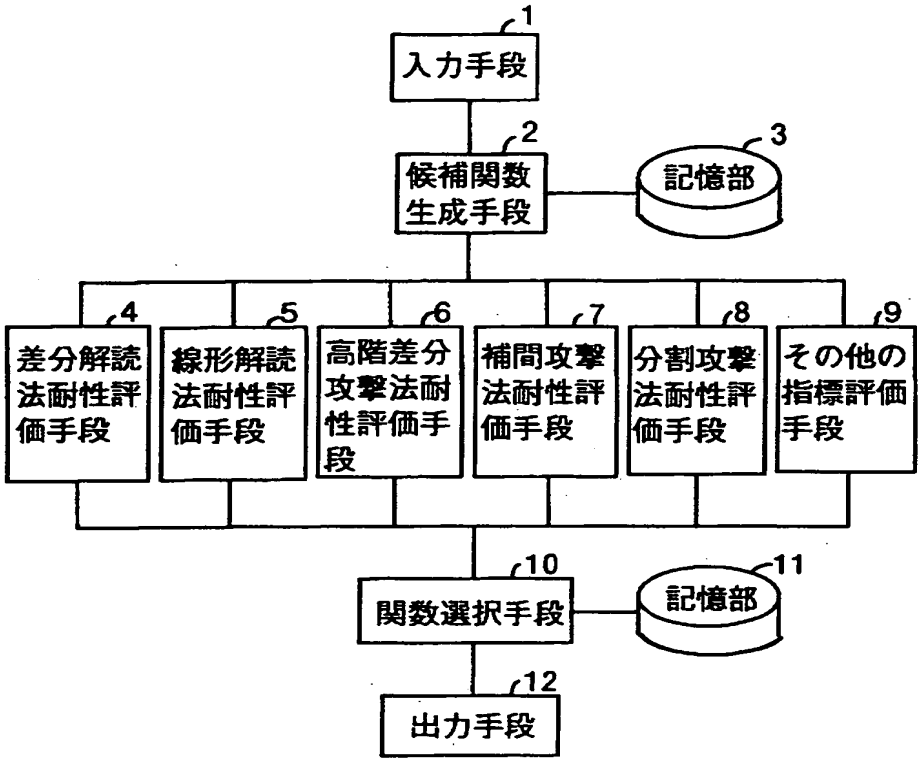

図　1

【図２】

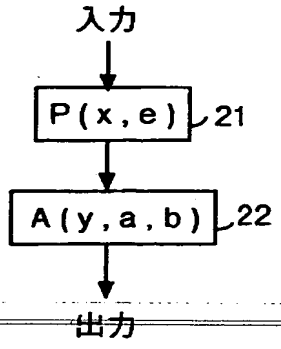

図　2

出証特平１１－３０４３０２１

【図３】

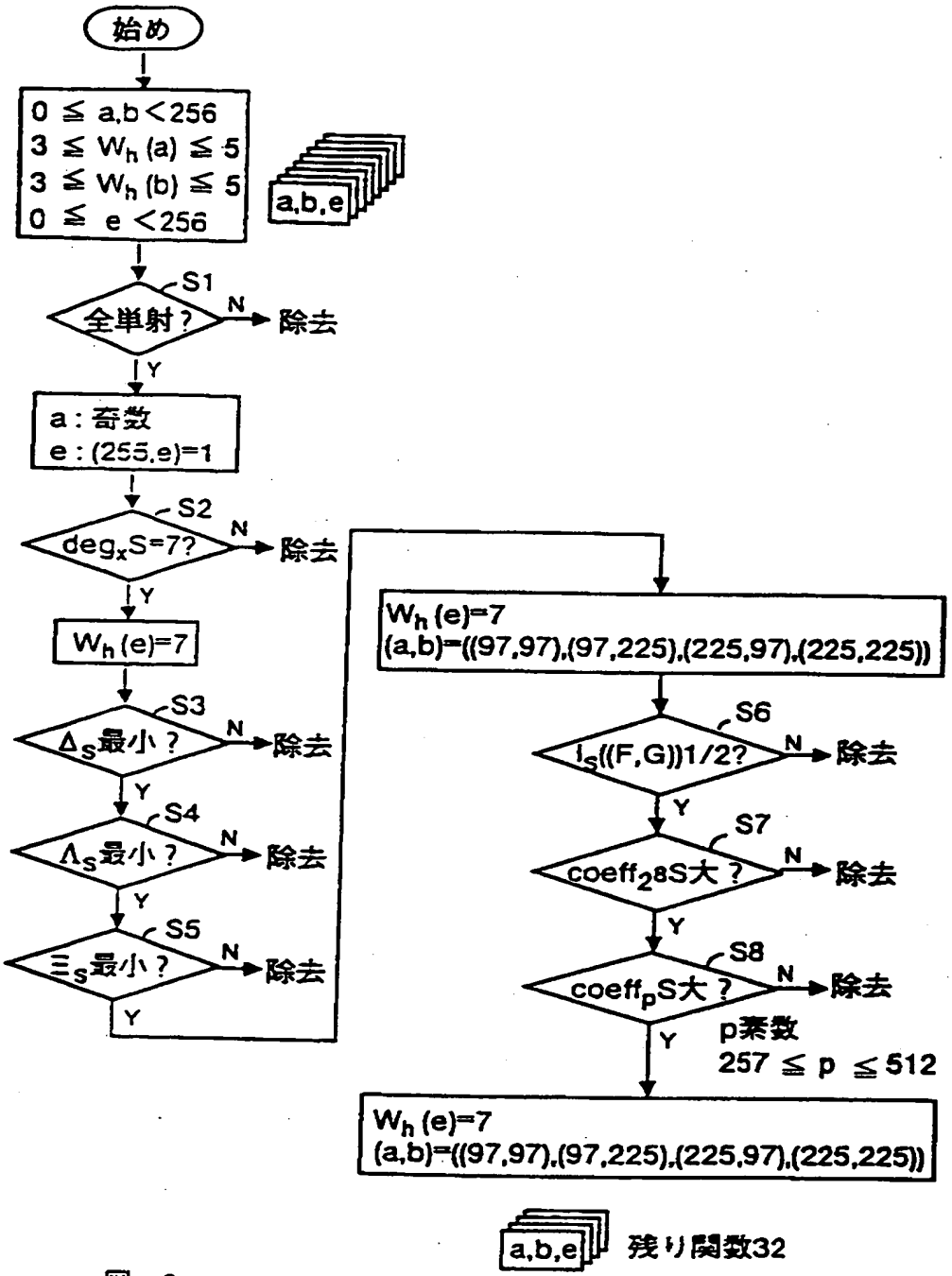
始め
0 ≦ a,b <256
3 ≦ Wh (a) ≦ 5
3 ≦ Wh (b) ≦ 5
0 ≦ e <256
a,b,e
S1
全単射？
N
除去
Y
a：奇数
e：(255,e)=1
S2
degxS=7?
N
除去
Y
Wh (e)=7
S3
ΔS最小？
N
除去
Y
S4
ΛS最小？
N
除去
Y
S5
ΞS最小？
N
除去
Y
Wh (e)=7
(a,b)=((97,97),(97,225),(225,97),(225,225))
S6
lS((F,G))1/2?
N
除去
Y
S7
coeff2S大？
N
除去
Y
S8
coeffpS大？
N
除去
Y
p素数
257 ≦ p ≦ 512
Wh (e)=7
(a,b)=((97,97),(97,225),(225,97),(225,225))
a,b,e
残り関数32

図 3

【書類名】　　要約書

【要約】

【課題】　差分解読法、線形解読法のみならず、高階差分攻撃法、補間攻撃法、分割攻撃法に対しても耐性が強い暗号化関数を生成する。

【解決手段】　$S=A((P(x, e)), a, b)$、$P(x, e)=x^{e}$ in $GF(2^{8})$、$A(y, a, b)=ay+b \pmod{2^{8}}$ を候補とし a，b のハミング重みを３以上５以下とし、a を奇数、e を２５５と互いに素とし（Ｓ１）、他の候補を除き、Ｓのブール多項式の次数 $\deg_x S$ が最大のものを選び（Ｓ２）、差分攻撃指標 Δ_S が最小のもの、線形攻撃指標 Λ_S が最小のものを選び（Ｓ３，Ｓ４）、更に差分線形攻撃指標 Ξ_S が最小のものを選び（Ｓ５）、分割攻撃指標 I_S （（F，G））が１／２に近いものを選び（Ｓ６）、補間攻撃指標が大きいものを選ぶ（Ｓ７，Ｓ８）。

【選択図】　　図３

出証特平１１－３０４３０２１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
　【識別番号】　000004226
　【住所又は居所】　東京都新宿区西新宿三丁目１９番２号
　【氏名又は名称】　日本電信電話株式会社
【代理人】　申請人
　【識別番号】　100066153
　【住所又は居所】　東京都新宿区新宿四丁目２番２１号　相模ビル
　【氏名又は名称】　草野　卓
【選任した代理人】
　【識別番号】　100100642
　【住所又は居所】　東京都新宿区新宿４丁目２番２１号　相模ビル　草野特許事務所
　【氏名又は名称】　稲垣　稔

出 願 人 履 歴 情 報

識別番号　〔０００００４２２６〕

１．変更年月日　１９９５年　９月２１日
［変更理由］　住所変更
住　所　東京都新宿区西新宿三丁目１９番２号
氏　名　日本電信電話株式会社